RESEARCH REVIEW JOURNALS
Volume-04
Issue-05
May-2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com[UGC Listed Journal]

Black hole Attack handling in Energy efficient way for Mobile Adhoc network

[1]Deepak Sharma and [2]Prashant Johri

[1]Associate Professor, Dept of Computer Science & Applications, Monad University
[2]Professor, Dept of Computer Applications, Galgotias University

ARTICLE DETAILS

Article History
Published Online: 25 May 2019

Keywords
Black-hole and gray-hole attack; digital signatures; intelligent routing protocol; MANET.

ABSTRACT

Energy and security are the two vital components of Mobile Ad-hoc Networks (MANETs). During routing finding an optimal path from sender to receiver sense of path length (number of hops), longevity (battery life) and security becomes an essential requirement. Variety of schemes are proposed by the researchers for finding the shortest path along with energy saving and protecting from attacks Black-hole and gray-hole attacks are some of the most harmful attacks against MANET communication and needs attention. These attacks may cause by insider or outsider malicious node(s) who may drop packets or misroute the information during communication from sender node to receiver node. In our study we proposed an intelligent routing protocol based on Ant Colony Optimization (ACO) technique that finds shortest path from source to destination, applies the concept of power aware techniques to save energy increasing the longevity of the link avoiding link failure and also uses the concept of digital signatures, watchdog and path rater for detection and avoidance of black- hole and gray-hole attacks. Simulation study of the proposed scheme is made over some network parameters and found to be efficient in comparison to the basic AODV routing protocol.

1. Introduction

Mobile Ad-Hoc Networks (MANETs) are autonomous deconcentrated frameworks or remote frameworks. In the system framework, MANETs consistently involves the mobile hubs which might be structures or subsystems, acting both as a switch and a host. Mobile hubs inside the system, contingent upon one another's association they can shape diverse system setup or geology by their self-plan power, with no fixed framework. Routing protocols are the most interesting, yearning and testing territories in MANET research. Specialists structured a number of routing protocols for MANETs, for example, AODV, DSR, DSDV, OLSR and so forth. The exceptionally serious concern for the essential functionality in MANET is vitality sparing and routing security. Mama NET hubs are battery fueled and during routing battery life augmentation is one of the measure issues in them. Finding a most limited way during routing brings about speedier exhaustion of battery life of partaking nodes. Due to the qualities, for example, open access medium, immovably changing system geography, lack of intermedial the board and observing frameworks, agreeable calculations and insufficiency of straightforward safeguard instrument of MANETs frequently poorly utilized by assailants and suffer security assaults. The system administrations openness, information honesty and classification can be picked up by protecting the security issues that have been recognized inside the system. Moreover, the wireless connection makes MANETs to be more susceptible to the attacks by providing access to on-going communications. Varieties of attacks are found out in the MANETs and classified as; worm-hole attack, black-hole attack, rushing attack, byzantine attack, resource consumption attack, location disclosure attack, sybil attack, flooding attack, Denial of Service (DoS), spoofing attack etc. [1].

Much energy aware routing schemes [2-8] are proposed in the literature. The Minimum Total Transmission Power Routing (MTPR) [2] computes the overall energy needed for transmitting the packets through various paths and finally chooses the one with minimum power required but the remaining power with nodes is not taken into consideration, which may lead to destruction of some nodes in the path resulting in path failure. Min-Max Battery Cost Routing (MMBCR) [3] computes the energy of each node in a path and selects the minimum power nodes in each path. Then the path having the node with maximum battery power among these minimum powered nodes is selected. MMBCR extends life-time of a network by choosing remaining energy of a node but neglects the consumption factor and total transmission energy. The Conditional Max-Min Battery Capacity Routing(CMMBCR)

[4] combine the factors total transmission energy and remaining energy of nodes under consideration. MTPR is applicable when all the participating nodes are above the threshold value fixed for battery protection, otherwise MMBCR is used. Minimum Drain Rate (MDR) [5] uses a metric drain rate which is computed for a node as a ratio of remaining energy and rate of energy consumption considering the ongoing traffic conditions. The path with minimum drain rate and minimum battery power is chosen. Antecedently, many more works are performed on issues of security. Black-hole attack is one of the most vulnerable type of attack which is deeply related to reactive routing protocols in MANET like AODV and DSR. In our work we condense or concentrate our study on the Blackhole attack and one of its special case known as gray-hole attack. We have proposed an energy aware solution for detection and avoidance of black-hole and grey-hole attacks on MANETs. The proposed scheme is analyzed and compared with basic AODV routing protocol through a simulation carried out using NS-2. Its consequences are explained by expressing the effect of this attack to interrupt the normal execution of MANET routing protocols.

2. Black-hole attack and gray-hole attack

In black-hole attack [9] attacker nodes exploit the susceptibility during route discovery process of reactive routing protocols and inject false route to the destination. On receiving a RRER message intermediate attacker node replies with a RREP having an excessive destination sequence number than the RREQ message received claiming to the destination. When an attacker chooses the concept of rushing along with high power transmission to make this attack. It is quite impossible to find out a route not passing through the attacker node. Once the node chosen as an intermediate node or becoming part of routes in the network starts misusing or discarding the traffic being directed by it building a black-hole. This situation turns severe when the attacker becomes the part of more number of routes.

Classification of black-hole attacks made according to the presence of attacker nodes such as:

i) Internal black-hole attack
ii) External black-hole attack

Similarly, classification of black-hole attacks can be done in an- other way based upon the collaboration among the attacker nodes such as:

i) Single black-hole attack
ii) Collaborative black-hole attack

2.1. Internal black-hole attack

To launch this type of attack an insider compromised node stays across the sender and receiver nodes, becomes the part of an active route and conducts the attack. Internal black-hole attacks are named so as the attacker node by self is a member of the current network in which data transmission is carried out. This type of attacks is more endangered to guard against as it is so difficult to detect the internal compromised nodes.

2.2. External black-hole attack

In this type of black-hole attack attackers remain exterior to the current network and decline access to the network traffic, disrupting the network or creating congestions as shown in Figure. Further the external black-hole attacks may lead to internal black-hole attack by compromising some of the internal legitimate nodes involving them in attacking other nodes in MANET.

2.3 Single black-holeattack

In this type of attack situations, a particular attacker node broad- casts itself for containing fresh routes towards the destination node following the shortest path and it helps the attacker node to reply all the RREQs being the part of route, further during data transfer intercepts the data packets and retaining it [11]. In reactive routing protocols that uses flooding mechanism a mischievous and forged route is created as the attacker nodes RREP is received before the legitimate ones. Being the part of route, the attacker node behaves to drop all the packets received or to send them for an arbitrary address [12]. Overall, we can say that to make a black-hole attack the attacker node becomes the part of the route but how it is not specified as it differs from protocol to protocol.

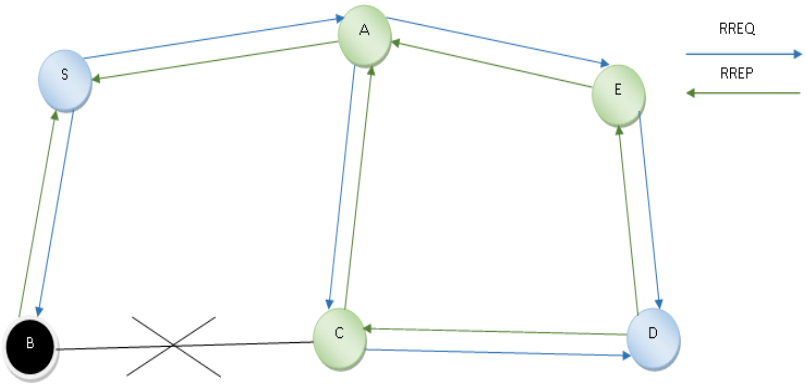

Fig. 1: Single black-hole Attack.

2.4. Cooperative black-hole attack

Some attackers perform in a class to launch this type of black-hole attacks. In Fig. 2, “S” and “D” represents the sender and receiver node respectively, nodes “A”, “B1”, “B2”, “C”, “E”, and “F” are the intermediate nodes. Considering “B1” and “B2” be the cooperative Black-hole nodes, when “S” want a data transmission to “D”, a route discovery is initiated by sending RREQ packets towards its neighbors.

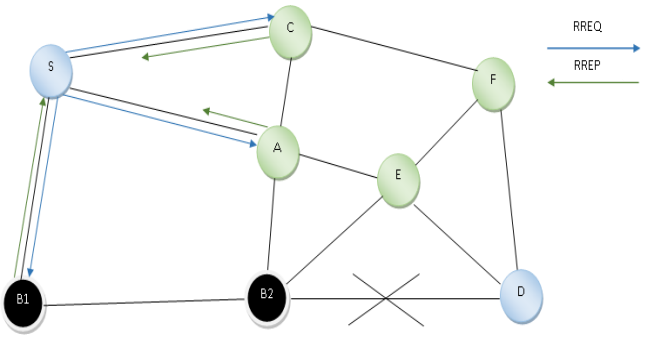

Fig. 2: Cooperative black-hole Attack.

3. Review of Literature

Black-hole attack is a measure security attack during routing and it needs a ton of regard for manage this issue. Analysts supportive of presented different security answers for manage this attack, yet our investigation incorporates some of them dependent on the works completed inside these ongoing years.

VishvasKshirsagar et al. [15] proposed an answer for dodge packet dropping by anode utilizing Bayes' Theorem and Prior likelihood strategy. At the point when a node found to drop packets, it is killed from the network. Utilizing this heuristic numerical model secure defeat ing can be conceivable utilizing a free situation.

GayatriWahane et al. [16] set forward an instrument for identification of agreeable black-hole attack dependent on crosschecking with a clock based system called TrueLink in AODV routing proto-col. Creators additionally led a reenactment to demonstrate the base routing overhead, postponement and greatest throughput with increment in attacker nodes and interruption time.

Ayesha Siddiqua et al. [17] recommended a strategy for identification and avoidance of the black-hole attack dependent on secure information calculation. The creators observed the information conveyed to recipient and investigated the explanations behind packet drops during correspondence dependent on which a node announced to be malevolent as a black-hole node.

NidhiChoudhary et al. [18] introduced a trust-based instrument for recognizing the black-hole node. A blacklist table is kept up at each node and trust estimation of its neighbor nodes is recorded. Trust estimation of any neighbor getting down the recently set limit esteem, the neighbor node are listed in the blacklist table primary tained.

Ali Dorri et al. [19] proposed a location strategy for black-hole attack in which next bounce and past jump node of a RREP packet is checked for the distinguishing proof of getting rowdy nodes in the way. Sener node recognizes a getting rowdy node by investigating the Data Routing Information table kept up by it.

J.M. Chang et al. [20] set forward a trap location approach for safeguarding against the cooperative attacks made by the pernicious nodes in MANETs. Black-hole attacks are distinguished and forestalled by structuring a Cooperative Bait Detection Scheme (CBDS) which gives the advantages of proactive protection designs just as reactive safeguard models utilizing a converse following procedure. Abdelshafy et al. [21]presented a strategy to distinguish noxious nodes by utilizing an idea of Self-Protocol Trustiness and another technique for opposing the black-hole attacks as Black-hole Resisting Mechanism which can be installed with any of the reactive routing protocols. The proposed techniques utilize nearby clocks and fixed limit esteems for arranging any node as malignant. Recreation examines are made utilizing NS-2 by the creators to show that the exhibition of the network increments by his supportive of presented work in contrast with AODV and SAODV under black-hole attacks.

Dixit et al. [22] recommended an interruption location framework dependent on casting a ballot to identify black-hole attack and dark hole attack in MA-NET. A routing table is kept up dependent on the votes made by the nodes taking an interest inside the network dependent on the conduct of their neighbor nodes. Nodes with higher vote numbers make the way for routing though negative democratic makes a node out from a functioning route.

4. Our proposal

Our framework uses an agent-based technique that relies on the ACO meta heuristics to find out the optimal path during routing, along with security is provided using digital signatures [23], watchdog and path rate mechanism [24] to prevent external and internal black-hole attacks respectively during communication.

Initially during network setup each mobile node registers itself with the network and assigned a private key, shared public key pair which is used by the individual mobile nodes for generation of digital signatures. Each node makes a neighbor discovery by using the HELLO messages. During communication each node selects the next hop using the metric next hop availability which can be described as a probabilistic value;

$$P_{(NH)} = (\Omega)^{\rho} / \Sigma((\Omega)^{\rho})$$

4.1 RouteDiscovery

Whenever a pair of nodes want to communicate with each other and no routing information is available with sender, then the source node creates a Forward Agent (FA) and attaches its own digital signature to it. Then the FA broadcasted to its neighbors. Each neighbor receiving a FA verifies its digital signature and finding it to be correct; the FA is accepted by the neighbor. Each intermediate node receiving a FA attaches its own digital signature to it and rebroadcasts to its neighbors until the destination node is reached. During its travel towards the destination, the FA's gather the path information with them.

Reaching the destination, the FA is killed and a Backward Agent (BA) is created which travels from the destination towards the source based upon the gathered information's by the FA. BA attached with the digital signature of the destination and forwarded towards the source. Any intermediate node receiving the BA verifies the digital signature and getting it to be correct accepts the BA. BA during its travel updates the pheromone table at a node in terms of remaining energy and hop count as described in EAAR [25].

$$\Omega = MBR / H$$

Any mismatch with the verification of digital signature leads to killing the FA or BA at the middle of communication. Repeating the process at every intermediate node BAs reach the source node. Reaching the source node BA's are killed and multiple successful paths are established.

4.2 Data transfer

Once the path discovery is over and successful routes are established between the source and destination, the data transfer process starts in between them. During data transfer digital signatures are also used with all the data packets sent to provide security during communication.

4.3 Route maintenance and linkfailures

Source node periodically undergoes verifying the paths by sending FA's and BA's in continuous intervals of time. In between any link failure due to removal of a malicious black-hole node or any other reason may be addressed by starting a new route discovery locally from the node where no further routing information are available.

4.4 Malicious nodedetection

At the point when an outside aggressor node needs to partake in the dynamic course it is discovered during digital signature check stage because of the inaccessibility of the mystery key with it, as the key is just present with the inward enrolled portable nodes as it were. For inside getting into mischief nodes, every portable node inside the network installed with a guard dog and way rater component so they can screen their neighbor nodes during information move. Each node screens its neighbors for the elements like information bundle misfortune, information moves rate and bogus flooding and so on. In the event that any of the elements goes be-low the base limit esteem, at that point the neighbor node put the node in the noxious node list and advises all the real nodes in the network about the vindictive conduct of the node by communicating a message.

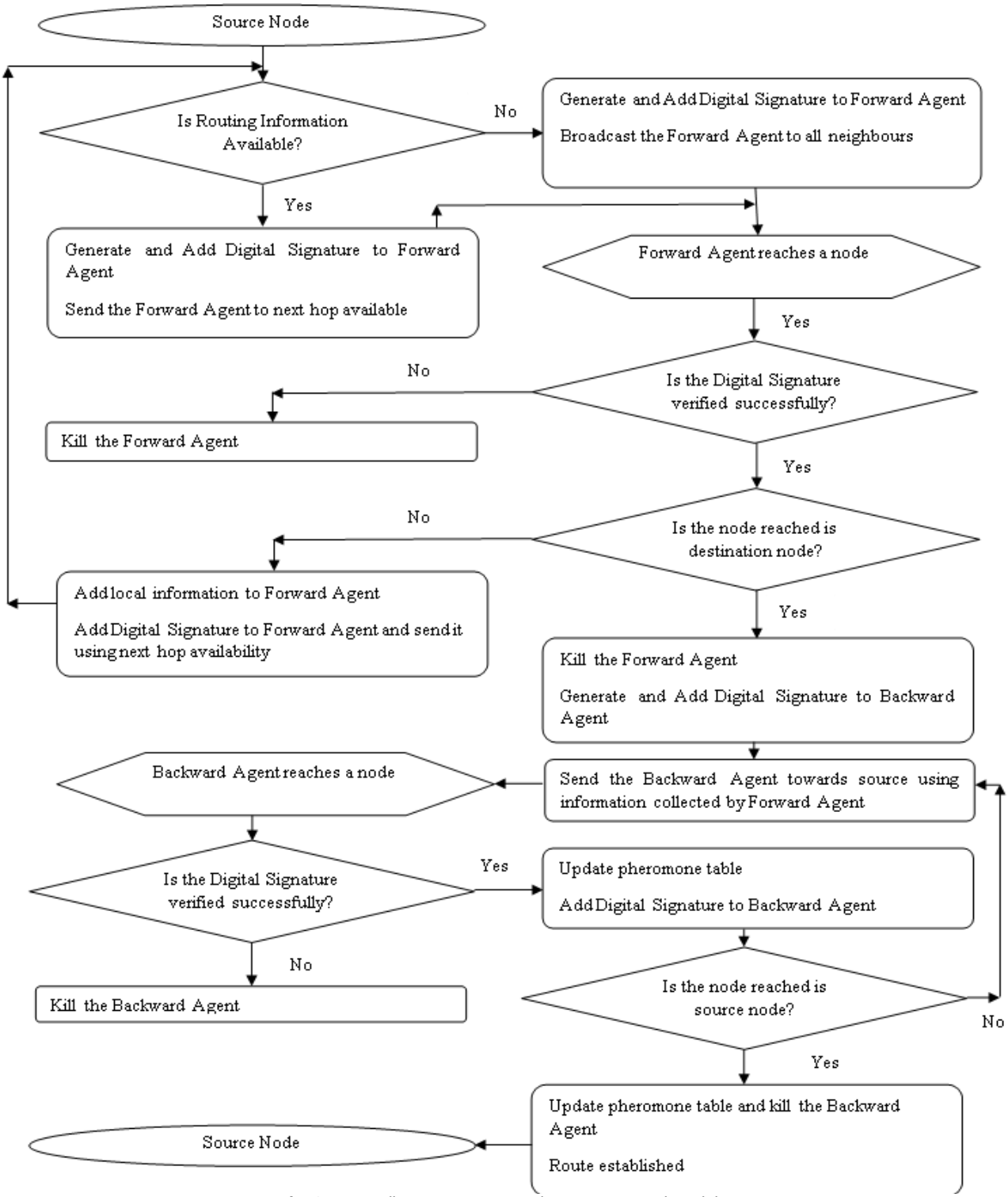

Fig. 3: Route discovery process using our proposed model.

5. Simulation and results

For the purpose of simulation modification is done to the existing AODV routing protocol according to our proposed routing methodology and compared with the basic AODV routing protocol. The simulation carried out using the network simulator NS-2.35. The view of complete simulation environment is represented in Table1.

We have used some of the simulation parameters like packet de- livery ratio and number of packets lost against the number of attackers. Parameters like routing overhead, network energy consumption and network throughputs are used against the simulation time for evaluation of performance of our proposed scheme in comparison to basic AODV routing protocol.

Table 1: Simulation scenario and parameter settings

Parameter Name	Value
Number of nodes	50
Node distribution	Random
Area dimension	1500 x 750
Simulation time	300 s
Propagation	Radio-propagation model
Network type	Wireless
Traffic generator	CBR
MAC type	IEEE 802.11
Data rate	11 Mbps
Antenna type	OmniAntenna
Mobility pattern	Random
Node speed	10 to 15 m/s
Interface queue type	DropTail/PriQueue
Max packet in interface queue	50

5.1. Packet delivery ratio (PDR)

PDR can be computed as a fraction of total number of data packets collected at the destination with respect to total number of packets sent by the constant bit rate (CBR) source. Performance of a net- work increases with the increase in packet delivery ratio values.

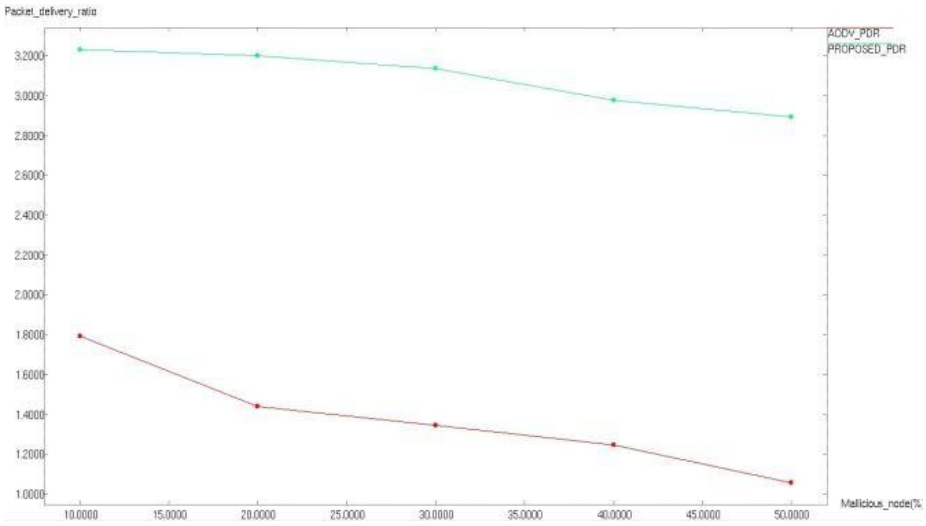

Fig. 4: Comparison graph showing packet delivery ratio.

4.2. Packet loss (PL)

PLcan be computed as a fraction of total number of packets lost due to congestion or any other reason with respect to total number of packets sent during transmission. Performance of a network increases with the decrease in packet loss values.

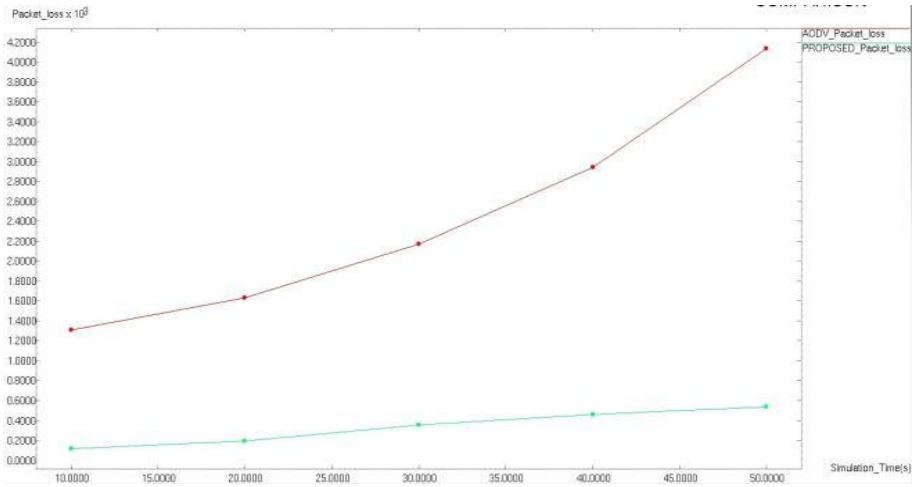

Fig. 5: Comparison graph showing number of packet lost.

4.2. Routing overhead (RO)

RO can be computed as a fraction of number of routing packet transmitted with respect to number of successfully delivered data packets where routing packets comprises control packets utilized for route discovery, route maintenance, and pheromone updates. Performance of a network increases with the decrease in routing packet overhead values.

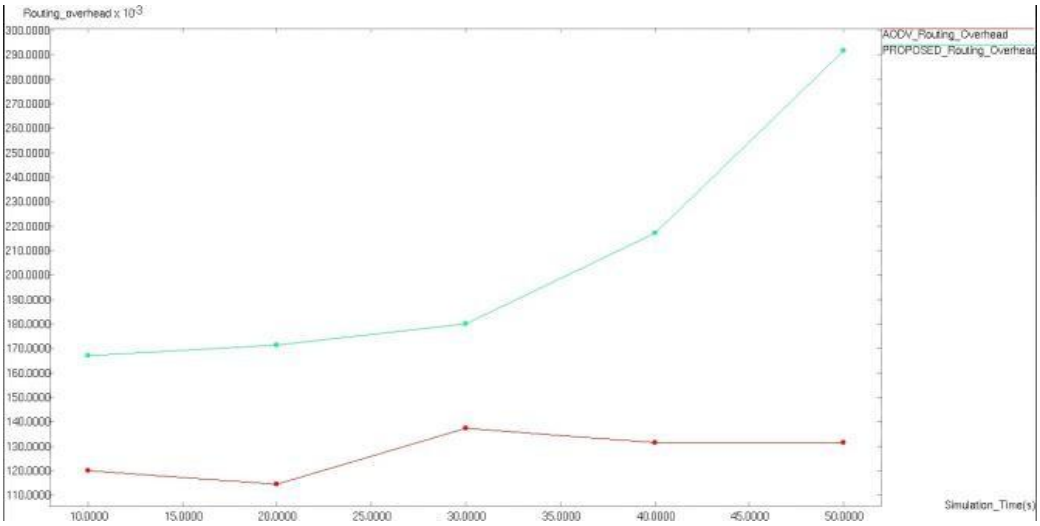

Fig. 6: Comparison graph showing routing packets overhead.

4.2. Energy consumption (EO)

EO is the part of energy spent by the nodes during receiving the packets from neighbor nodes and transmitting the packets to neighbor nodes. Performance of a network increases with the de- crease in energy consumption values.

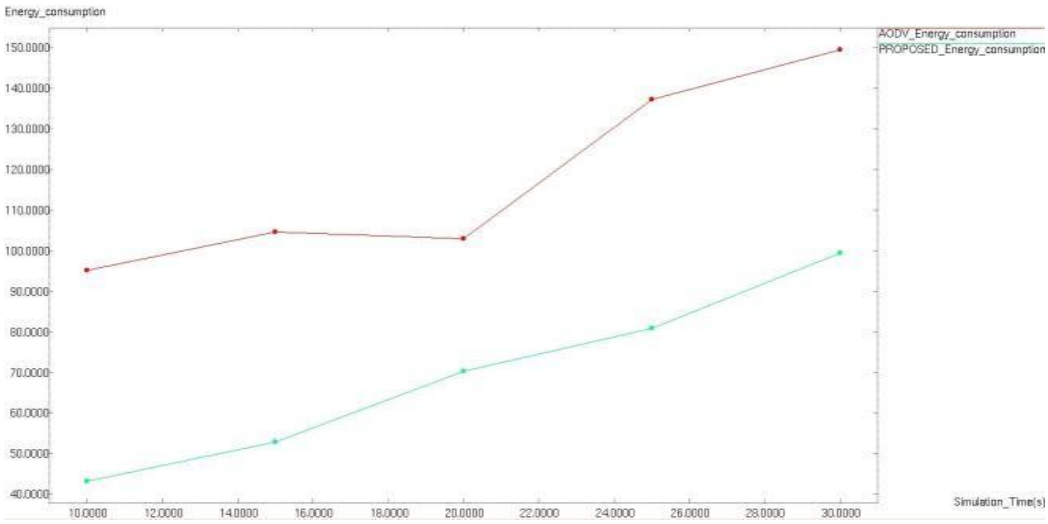

Fig. 7: Comparison graph showing average energy consumption.

4.2. Network throughput (NT)

NT can be compute as a ratio of the amount of packets moved successfully from sender to receiver within a particular time period and represented in bps. Performance of a network increases with the increase in throughput values.

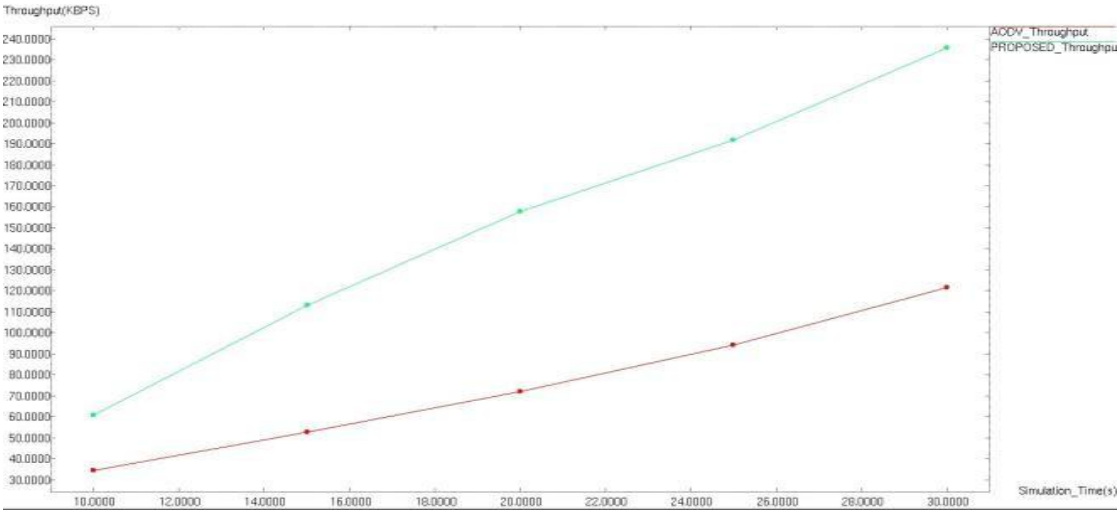

Fig. 8: Comparison graph showing network throughput.

6. Conclusion

In this paper we have initialized our study with the basic idea of MANET and need of power aware secure routing features in MANET. Then we discussed about the most repeated attacks in MANET known as black-hole and gray-hole attacks. We discussed about some of the solution proposed by various researchers. A multipath intelligent routing protocol is proposed for finding an optimal path from sender to receiver along with increasing the lifetime of the network and providing security against these attacks. We analyzed the effect of these attacks by simulation studies on the network parameters network routing load, network throughput, packet delivery ratio, packet loss and network energy consumption using our proposed energy aware secure routing protocol and the base AODV routing protocol. Implementations show that our proposed work detects and avoids the attacks more efficiently in comparison to basic AODV and increases network performance but increase in network routing load is also seen with increase in number of attackers.

References

1. Pankajini Panda, Khitish Ku. Gadnayak, Niranjan Panda, “MA- NET Attacks and their Countermeasures: A Survey”, Interna- tional Journal of Computer Science and Mobile Computing (IJCSMC), vol. 2, no. 11, pp. 319-330,2013.
2. Scott, K., Bambos, N., 1996. Routing and channel assignment for low power transmission in PCS. In: Proc. Intl. Conf. Univer- sal Personal Communications (ICUPC’96), Cambridge, MA, pp. 498–502.
3. Singh, S., Woo, M., Raghavendra, C.S., 1998. Power-aware rout- ing in mobile ad hocnetworks. In: Proc. 4th Annual ACM/IEEE Intl. Conf. Mobile Computing and Networking, Dallas, TX, pp. 181–190.
4. Toh, C.-K., 2001. Maximum battery life routing to support ubiq- uitous mobile computing in wireless ad hoc networks”. IEEE Communications Magazine 39 (June (6)),138–147.
5. Kim, J., Garcia-Luna-Aceves, J., Obraczka, K., Cano, J.-C., Manzoni, P., 2002. Power aware routing based on the energy drain rate for mobile ad hoc networks. In: Proc. 11th Intl. Conf. Comp. Comm. Netw., pp.565–569.
6. Liang, W., Yuansheng, Y., 2004. Maximizing battery life routing in wireless ad hocnetworks. In: Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii,USA.
7. Srinivas, A., Modiano, E., 2005. Finding minimum energy disjoint paths in wireless ad-hoc networks. Wireless Netw. 11, 401– 417.
8. Yuen, W.H., Sung, C.W., 2003. On energy efficiency and net- work connectivity of mobile ad hoc networks. In: Proc. 23rd IEEE Intl. Conf. Distrib. Comput. Sys. (ICDCS’03), Rhode Is- land, May 2003, pp.38–45.
9. Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." *Proceedings of the 42nd annual Southeast regional conference*. ACM,2004.
10. M. Chaitanya Kishore Reddy and BoyaSripriya, “A Study on Gray-hole Attacks in Mobile Ad-hoc Networks”, 2017 Interna- tional Journal of Advance Technology and Innovative Research, vol 9, pp. 1634-1636,2017.
11. Biswas, Kamanashis, and Md Ali. "Security threats in mobile ad hoc network."(2007).
12. Pequeño, Guillermo Alonso, and Javier Rocha Rivera. "Exten- sion to MAC 802.11 for performance Improvement in MANET." (2007).
13. Deng, Hongmei, Wei Li, and Dharma P. Agrawal. "Routing se- curity in wireless ad hoc networks." *IEEE Communications magazine* 40.10 (2002):70-75.
14. VishvasKshirsagar, Ashok M. Kanthe, and Dina Simunic “Ana- lytical approach towards packet drop attacks in mobile ad-hoc networks,” IEEE International Conference on Computational In- telligence and Computing Research

(ICCIC), IEEE,2014.

15. GayatriWahane, Ashok M. Kanthe, and Dina Simunic, “Detection of cooperative black hole attack using cross checking with truelink in MANET,” International Conference on. Computa- tional Intelligence and Computing Research (ICCIC), IEEE, 2014.
16. Ayesha Siddiqua, KotariSridevi, and Arshad Ahmad Khan Mo- hammed, “Preventing black hole attacks in MANETs using se- cure knowledge algorithm,” International Conference on Signal Processing and Communication Engineering Systems (SPACES), IEEE, 2015.
17. NidhiChoudhary, and LokeshTharani, “Preventing black hole attack in AODV using timer-based detection mechanism,” Inter- national conference on Signal processing and communication engineering systems (SPACES), IEEE,2015.
18. Ali Dorri and HamedNikdel, “A new approach for detecting and eliminating cooperative black hole nodes in MANET,” 7th Con- ference on Information and Knowledge Technology (IKT), IEEE, 2015.
19. Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, HanChieh Chao, and Chin-Feng Lai, Member, IEEE "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Co- operative Bait"(2015)
20. M. A. Abdelshafy and P. J. B. King, "Resisting blackhole attacks on MANETs," 2016 13th IEEE Annual Consumer Communica- tions& Networking Conference (CCNC), Las Vegas, NV, 2016, pp.1048-1053.
21. S. Dixit, P. Pathak and S. Gupta, "A novel approch for gray hole and black hole detection and prevention," 2016 Symposium on Colossal Data Analysis and Net-working (CDAN), Indore, 2016, pp.1-6.
22. Harn, Lein, Manish Mehta, and Wen-Jung Hsin. "Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA)." IEEE Communications Letters 8.3 (2004):198-200.
23. Marti, Sergio, et al. "Mitigating routing misbehavior in mobile ad hoc networks." Proceedings of the 6th annual international conference on Mobile computing and networking. ACM,2000.
24. Misra, Sudip, et al. "An ant swarm-inspired energy-aware rout- ing protocol for wireless ad-hoc networks." Journal of systems and software 83.11 (2010):2188-2199.

